EA C451
Internetworking Technologies
Second Semester 2012-13

CONSTRAINED-DHCP PROTOCOL

BITS Pilani
K K Birla Goa Campus

Submitted By

Tanushree Bansal 2010C6PS656G

Mrunal Mozarkar 2010C6PS527G

BITS, Internetworking Project
Internet-Draft
Intended status: Informational
Expires: October 16, 2013

M. Mozarkar
T. Bansal
BITS
April 14, 2013

Constrained DHCP Protocol
C-DHCP Protocol

Abstract

The Dynamic Host Configuration Protocol (DHCP) is a standard protocol defined by RFC 2131 which allows a server to dynamically distribute IP address and configuration parameters to clients. The constrained DHCP protocol encompasses only a part of the functionality of the standard DHCP protocol. The constrained-DHCP server provides the client with either or both of the following:

1. IP Address

2. Subnet Mask

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 16, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

The constrained-DHCP uses dynamic allocation mechanism where the server assigns the IP address to the requesting client for an unlimited period of time. The client will explicitly have to inform the server to relinquish the IP address allocated to it. Thus this protocol allows the reuse of addresses that has been relinquished by host. This is especially valuable since the pool of available IP addresses is limited (25 in number).

The constrained-DHCP protocol uses client-server architecture. The client sends a broadcast request for configuration information. The constrained-DHCP server receives the request and responds with configuration information from its database. This protocol involves the exchange of DHCP messages between the client and the server during the address allocation sequence. This is a four step process that includes discover (broadcast), offer (broadcast), request (unicast) and finally acknowledgement(broadcast). The client need not know the address for DHCP server to initiate its requests for configuration information.

The format of constrained-DHCP messages is based on format of standard DHCP messages with some of the fields pertaining to relay agents removed. The complete message format is explained in Section 2

1.1. Problem Definition and Scope

Constrained-DHCP protocol allows a client to request an IP address and/or the subnet mask from the DHCP server. The client can request one or both the fields depending upon the OP field of the constrained-DHCP message.

The server will not give the IP address on lease. Only when the client wants to release its IP address, it will inform the server.

The constrained-DHCP server will use the transaction-id of the constrained-DHCP message and the hardware address of the client as a key to store the information about the parameters allocated to each client.

The constrained DHCP-Protocol consists of two types:-

DHCP Server: The server will be configured with the following parameters:

1. A range of Class C IP addresses (maximum 25 in number)

2. Subnet Mask: There are two subnets and each client will be allocated one subnet mask(if the client requests for it).

The constrained-DHCP server accepts the constrained-DHCP packet, and allocates the fields requested in it, using the same packet structure. If there is no IP address available to be allocated, it informs the client in the same packet.

DHCP Client: Several clients can ask for an IP address and/or subnet mask. It is done by setting the fields of the DHCP message and sending the packet to DHCP server. It can also release the IP address voluntarily. It is assumed that there is no router between the clients and server and they can communicate directly. The constrained- DHCP protocol is not intended to be used for configuration of routers.

1.2. Terminology

This document uses the following terms:

Constrained-DHCP Client: It is an Internet host using the constrained-DHCP protocol to obtain configuration parameters such as a network address and/or a subnet mask.

Constrained-DHCP Server: It is an Internet host that returns configuration parameters to the constrained-DHCP clients.

2. Message Structure

Constrained-DHCP provides configuration parameters to a maximum of 25 internet hosts. The message format is based on the DHCP message format as given in RFC 2131 with certain modifications made.

2.1. Constrained-DHCP Message Format

The constrained-DHCP message format is shown in figure 1. The numbers in the parenthesis indicate the size of each field in bytes.

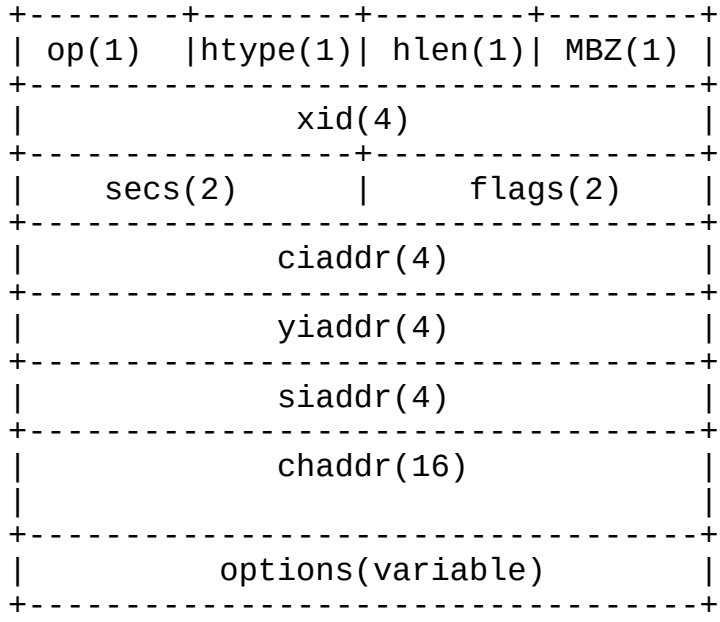


Figure 1: Format of a constrained-DHCP message

The following table(Table 1)describes each of the fields in the above message format-

Fields	Octet	Description
op	1	Message op code (figure 2)
htype	1	Hardware address type
hlen	1	Hardware address length
xid	4	Transaction ID(a random number chosen by the client and server to associate messages and responses between a client and a server)

secs	2	Filled in by the client. It is the seconds elapsed since client began address acquisition or renewal process.
flags	2	Only the first bit is used; called the broadcast bit; Rest bits set to zero
ciaddr	4	client iP address; filled in by client only when its network address is known to be valid.
yiaddr	4	'your' client IP address
siaddr	4	Sever puts in its IP address during DHCP offer
chaddr	16	Client Hardware address
options	variable	Optional Parameters field

Table 1: Description of fields in a DHCP message

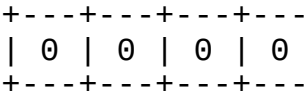


Figure 2: Op Field in Constrained-DHCP meassage

Op-Bits	Value
SB	=1(if the client requests for subnet) =0(otherwise)
IP	=1(if the client requests for an IP address) =0(otherwise)
RP	=1(if the reply is sent by the server) =0(otherwise)
RQ	=1(if the request is sent by the client) =0(otherwise)

Table 2: Op Field Explanation

The first four octets of the ’options’ field of the constrained-DHCP message contain the decimal values 99, 130, 83 and 99 respectively(magic cookie). The remainder of ’options’ field consists a list of tagged parameters called "options".The Constrained-DHCP options include the message type(for example type 1 refers to DHCPDISCOVER message),subnet mask if requested by the client. The last option must always be the "end" option.

2.2. Fields Removed

The constrained-DHCP message format contains lesser number of fields as compared to standard DHCP message format. The following fields have been removed-

Hops: Client sets this field to zero and it is optionally used by relay agents. Since in this case the server and client are directly connected and relay agents do not come into picture, this field is replaced by MBZ(Must be zero).

giaddr: IP address of the next server used in bootstrap is stored in ’giaddr’, but the constrained DHCP protocol is designed only for one server, hence this field is rendeered unnecessary.

sname: It contains an optional server host name.

file: This field contains the boot file name(optional); fully qualified path name on host with IP address siaddr; used in Boot Protocol to specify boot file for client.

The last 2 fields above are not required for the functioning of the constrained-DHCP protocol and hence have been removed.

3. Main Policies

The client-server interactions in the constrained-DHCP protocol occur in a similar manner as that of the standard DHCP protocol. The main policies are mentioned below-

1. The constrained-DHCP client can only ask for an IP address and/or a subnet mask from the constrained-DHCP server and no other configuration parameters. The parameters requested by the client are indicated by setting the bits of the OP field(as explained in Section 2.1)

2. The constrained-DHCP client will initially broadcast a DHCPDISCOVER message in its local subnet. The constrained-DHCP server will accept this DHCP packet and will offer the fields requested in it. This will be done via the DHCPOFFER message.The

client receives this packet and requests for the IP address using DHCPREQUEST message.The server will then allocate the fields requested in it. It will inform the client using the same packet structure via the DHCPACK message. If there is no free IP address to be allocated, a DHCPNACK message will be sent by the server to inform the client.Thus, the client and server interact in a four step manner.

3. A DHCPNACK will also be sent in response to the DHCPDISCOVER message by the client in the following two cases:

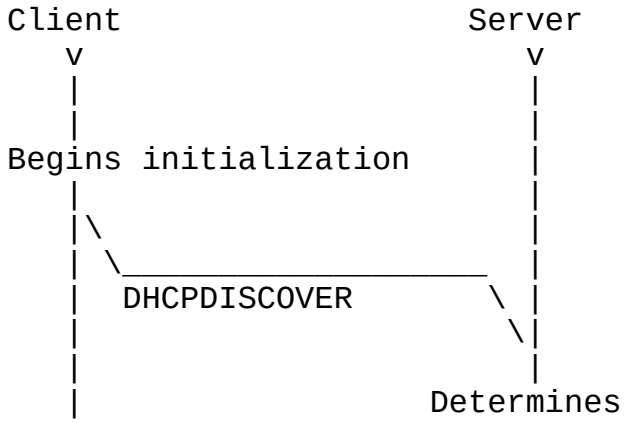
    1. The client asks for a subnet mask without having an IP address allocated to it.

    2. The IP address of the client does not lie in either of the subnets of the constrained DHCP server.

4. The address will be dynamically allocated to the constrained-DHCP client for an unlimited amount of time. So, time value in the options filed is alwys set 0xffffffff to represent infinity. When the client wants to release the IP address, it will inform the server using the DHCPRELEASE message.

5. The constrained-DHCP server stores information of parameters allocated to various clients using the transaction is (xid) and the hardware address of the client as a key. Whereas the standard DHCP protocol uses a combination of xid and the allocated ip address as a key to store configuration information.

6. There will be only one constrained-DHCP server in the network with no routers between the server and client allowing direct communication between them. So, all the policies related to relay agents are not present as part of this protocol. The fields pertaining to relay agents in the message format have been removed(as explained in Section 2.2)



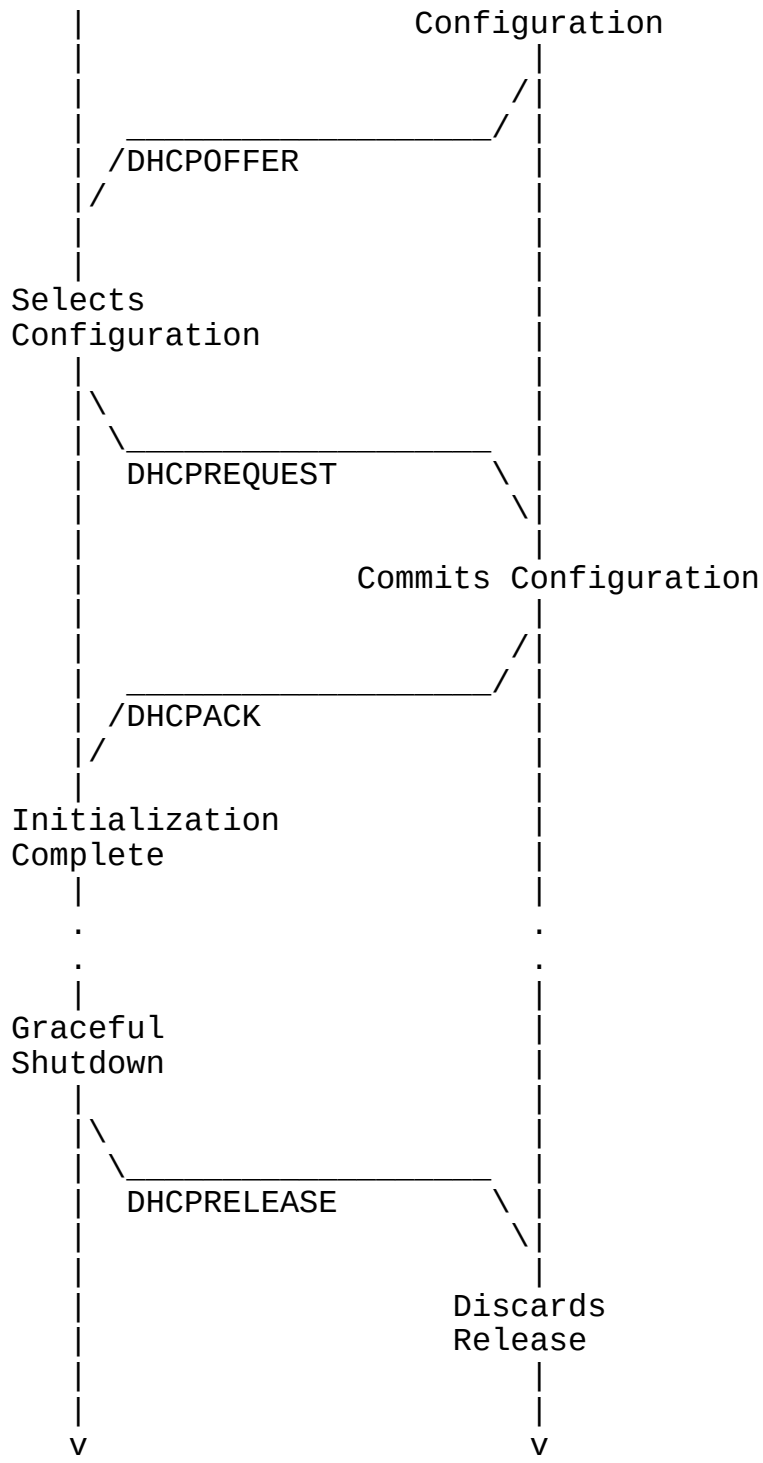


Figure 3: Timeline diagram of messages exchanged between DHCP client and servers when allocating a new network address

4. Technologies used for the implementation

The following section gives details of the technology/programming language used to implement the constrained-DHCP protocol and the various data structures used to store information at the server end.

4.1. Programming Language-JAVA

Since Java was designed with networking in mind, network programming in Java is simpler as compared to other languages. In Java, the part of program that deals with network is always short and simple. It is essay for a java application to send and receive data and also to communicate over the internet. Java provides basic socket classes to make programming with sockets much easier. Hence, Java has been used to implement this protocol.

4.2. Data Structures

Data structures are required to maintain a pool of available IP addresses and for storing the parameters allocated to the clients. The data structures used are:-

Linked List: For maintaining a list of available IP address(Free ipPool). Linked list is used to avoid repetition of offering the same IP address during DHCPOFFER stage.This is done by putting the offered IP address at the end of the linked list. The next IP address offered is always the one that is present at the start of the list. A particular IP address is removed from the list only when it is assigned to some client.

HashMap: For storing allocated parameters with transaction ID and hardware address as key.

Stored parameters include allocated IP address and subnet mask(if given by server).

5. References

Appendix A. Informative References

RFC2131 is required to support the contsrained-DHCP protocol.

Authors' Addresses

Mrunal Mozarkar
BITS
CH-4
Goa
India

Phone: 96 04 47 63 34
Email: m.mozarkar@gmail.com

Tanushree Bansal
BITS
CH-4
Goa
India

Phone: 83 90 75 32 53
Email: tanushree656@gmail.com